

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-261265

(43)Date of publication of application : 03.10.1997

(51)Int.Cl.

H04L 12/46

H04L 12/28

G06F 13/00

H04L 12/56

(21)Application number : 09-006553

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 17.01.1997

(72)Inventor : INOUE ATSUSHI
ISHIYAMA MASAHIRO
MORIYA OSAMU
SHINPO ATSUSHI
OKAMOTO TOSHIO

(30)Priority

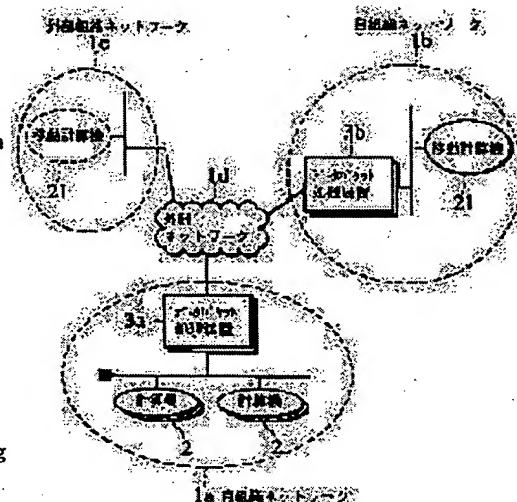
Priority number : 08 5886 Priority date : 17.01.1996 Priority country : JP

(54) COMMUNICATION CONTROL METHOD, REPEATER AND DATA PACKET PROCESSOR

(57)Abstract:

PROBLEM TO BE SOLVED: To attain flexible address control and management even when a computer making communication by moving on a network is moved to any position.

SOLUTION: When a mobile computer is located in a home network, the computer transfers communication data based on a 1st position identifier decided uniquely in its own organization network 1a, and when the mobile computer is located in an external own organization network 1b, the computer makes routing to the external own organization network based on a 3rd position identifier decided uniquely in the entire network denoting a moving position on a communication network. When the mobile computer is located in an external own organization network, the computer makes addressing based on the 1st position identifier and when the mobile computer is located in an external other organization network 1c, the computer makes routing to the external other organization network based on the 3rd position identifier, and when the mobile computer moves to the outside of the own organization network in the external other organization network, the computer makes addressing based on a 2nd position identifier rented for the mobile computer and decided uniquely in the entire network and makes communication.



LEGAL STATUS

[Date of request for examination]

30.10.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3464358

[Date of registration]

22.08.2003

[Number of appeal against examiner's decision of

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-261265

(43)公開日 平成9年(1997)10月3日

(51)Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 12/46			H 0 4 L 11/00	3 1 0 C
12/28			G 0 6 F 13/00	3 5 5
G 0 6 F 13/00	3 5 5		H 0 4 L 11/00	3 1 0 B
H 0 4 L 12/56		9466-5K	11/20	1 0 2 Z

審査請求 未請求 請求項の数23 O L (全 21 頁)

(21)出願番号 特願平9-6553

(22)出願日 平成9年(1997)1月17日

(31)優先権主張番号 特願平8-5886

(32)優先日 平8(1996)1月17日

(33)優先権主張国 日本 (J P)

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 井上 淳

神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内

(72)発明者 石山 政浩

神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内

(72)発明者 森谷 修

神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内

(74)代理人 弁理士 三好 秀和 (外3名)

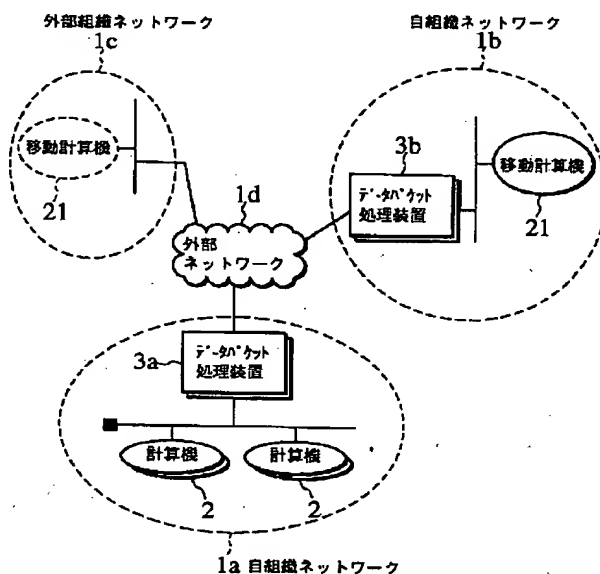
最終頁に続く

(54)【発明の名称】 通信制御方法、中継装置およびデータパケット処理装置

(57)【要約】 (修正有)

【課題】 ネットワーク上を移動しながら通信する計算機がどのような位置に移動しても柔軟なアドレス制御および管理を可能にする。

【解決手段】 移動計算機がホームネットワーク内に位置するときには、自組織ネットワーク1a内で一意に定める第1の位置識別子により通信データを転送し、外部自組織ネットワーク1b内に位置するときには、通信ネットワークシステム上の移動位置を示すネットワーク全体で一意に定める第3の位置識別子により外部自組織ネットワークにルーティングする。外部自組織ネットワーク内では第1の位置識別子によりアドレッシングし、外部他組織ネットワーク1c内に位置するときには、第3の位置識別子により外部他組織ネットワークにルーティングし、外部他組織ネットワーク内では自組織外に移動する際に移動計算機に貸し与えられるネットワーク全体で一意に定める第2の位置識別子によりアドレッシングし、通信を行う。



【 特許請求の範囲】

【請求項1】 複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能な通信ネットワークシステムにおいて、該複数の計算機のうち少なくとも一つの計算機が通信ネットワークシステム上の位置を変更しながら通信を行う移動計算機であるときの通信制御方法であって、

(a) 前記移動計算機がそのホームネットワーク内に位置するときには、該移動計算機に固有な該移動計算機の自組織ネットワーク内で一意に定められた第1 の位置識別子により通信データを転送して該移動計算機に対する通信を行い、

(b) 前記移動計算機が外部自組織ネットワーク内に位置するときには、該移動計算機の通信ネットワークシステム上の現在の移動位置を示すネットワーク全体で一意に定められた第3 の位置識別子により通信データを該外部自組織ネットワークにルーティングし、該外部自組織ネットワーク内では前記第1 の位置識別子により該移動計算機をアドレッシングして該移動計算機に対する通信を行い、

(c) 前記移動計算機が外部他組織ネットワーク内に位置するときには、前記第3 の位置識別子により通信データを該外部他組織ネットワークにルーティングし、該外部他組織ネットワーク内では該移動計算機が自組織外に移動する際に該移動計算機に貸し与えられるネットワーク全体で一意に定められた第2 の位置識別子により該移動計算機をアドレッシングして該移動計算機に対する通信を行う、
ことを特徴とする通信制御方法。

【請求項2】 互いに対応する前記第1 の位置識別子、前記第2 の位置識別子、前記第3 の位置識別子の組を含んだ前記移動計算機のアドレス情報を前記自組織ネットワーク内で管理することを特徴とする請求項1 記載の通信制御方法。

【請求項3】 通信相手計算機が前記自組織ネットワーク内に位置するときには、該通信相手計算機から通信データを前記移動計算機の前記第1 の位置識別子を付けて送信し、

前記移動計算機が前記外部自組織ネットワーク内または前記外部他組織ネットワーク内に位置するときには、前記ホームネットワーク内に設けられた中継装置において前記通信データに付けられた前記第1 の位置識別子に対応する前記第3 の位置識別子を前記アドレス情報に基づいて求め、該通信データに該第3 の位置識別子を付けて該中継装置から該移動計算機の現在の移動位置へ転送する、

ことを特徴とする請求項2 記載の通信制御方法。

【請求項4】 通信相手計算機が前記自組織ネットワーク外に位置するときには、該通信相手計算機から通信データを前記移動計算機の前記第2 の位置識別子を付けて

送信し、

前記移動計算機が前記外部自組織ネットワーク内または前記外部他組織ネットワーク内に位置するときには、前記ホームネットワーク内に設けられたデータパケット処理装置において前記通信データに付けられた前記第2 の位置識別子に対応する前記第3 の位置識別子を前記アドレス情報に基づいて求め、該通信データに該第3 の位置識別子を付けて該データパケット処理装置から該移動計算機の現在の移動位置へ転送する、

ことを特徴とする請求項2 記載の通信制御方法。

【請求項5】 前記管理するステップは、前記アドレス情報に対応してアドレス情報の有効期限を管理し、該有効期限が過ぎたときに該アドレス情報を無効化することを特徴とする請求項2 記載の通信制御方法。

【請求項6】 前記管理するステップは、新たな移動位置に移動した前記移動計算機から新たな第3 の位置識別子の登録を要求するメッセージを受け取り、該メッセージに含まれた署名情報にもとづいて該移動計算機が正しく認証されたときに、前記アドレス情報の前記第3 の位置識別子を書き換えることを特徴とする請求項2 記載の通信制御方法。

【請求項7】 前記管理するステップは、前記移動計算機から該移動計算機の切断を要求するメッセージを受け取ったときに前記アドレス情報を無効化し、該アドレス情報の無効化を該移動計算機に通知することを特徴とする請求項2 記載の通信制御方法。

【請求項8】 前記第3 の位置識別子は、移動計算機が移動先ネットワークで獲得したネットワーク全体で一意に定められた位置識別子であることを特徴とする請求項1 記載の通信制御方法。

【請求項9】 前記第3 の位置識別子は、前記ホームネットワーク外に移動した前記移動計算機を直接管理し該移動計算機と通信相手計算機との間の通信データを中継する外部中継装置を示し、ネットワーク全体で一意に定められた位置識別子であることを特徴とする請求項1 記載の通信制御方法。

【請求項10】 前記外部中継装置は、前記第3 の位置識別子に基づいて転送された通信データを受け取り、該通信データに付けられた前記第1 の位置識別子または前記第2 の位置識別子に基づいて該通信データを前記移動計算機に送ることを特徴とする請求項9 記載の通信制御方法。

【請求項11】 通信相手計算機が前記自組織ネットワーク内に位置するときには、該通信相手計算機から前記第1 の位置識別子を付けて前記通信データを送信し、前記通信相手計算機が前記自組織ネットワーク外に位置するときには、該通信相手計算機から前記第2 の位置識別子を付けて前記通信データを送出することを特徴とする請求項1 記載の通信制御方法。

【請求項12】 前記移動計算機が前記自組織ネットワ

10

20

30

40

50

3

ーク内に位置するときには、該移動計算機から前記第1の位置識別子をソースアドレスとして前記通信データを送信し、前記移動計算機が前記自組織ネットワーク外に位置するときには、該移動計算機から前記第2の位置識別子をソースアドレスとして前記通信データを送信することを特徴とする請求項1記載の通信制御方法。

【請求項13】 複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能な通信ネットワークシステムで、該複数の計算機のうち少なくとも一つの計算機が通信ネットワークシステム上の位置を変更しながら通信を行う移動計算機である通信ネットワークシステムにおいて、前記移動計算機のホームネットワークに設けられて通信データを中継する中継装置であって、

前記移動計算機に固有な該移動計算機の自組織ネットワーク内で一意に定められた第1の位置識別子と、該移動計算機に予約されたネットワーク全体で一意に定められた第2の位置識別子と、該移動計算機の通信ネットワークシステム上の現在の移動位置を示すネットワーク全体で一意に定められた第3の位置識別子と、の対応する組を含んだ前記移動計算機のアドレス情報を前記自組織ネットワーク内で管理する管理手段と、送信元計算機から送信された通信データに付加された前記第1の位置識別子または前記第2の位置識別子に対応する前記第3の位置識別子を前記アドレス情報から求め、得られた前記第3の位置識別子を前記通信データに付加して前記宛先計算機に向けて転送する処理手段と、を有することを特徴とする中継装置。

【請求項14】 前記自組織ネットワークに属する移動計算機に予約された複数の位置識別子を管理し、外部他組織ネットワークに移動する各移動計算機に前記複数の位置識別子の一つを前記第2の位置識別子として貸し出す手段を有することを特徴とする請求項13記載の中継装置。

【請求項15】 前記移動計算機が外部自組織ネットワーク内に位置し前記通信データの宛先が前記第1の位置識別子により指定されているときには、前記処理手段は該第1の位置識別子を含む該通信データを該第1の位置識別子に対応する前記第3の位置識別子でカプセル化し、前記外部自組織ネットワークに転送することを特徴とする請求項13記載の中継装置。

【請求項16】 前記移動計算機が外部他組織ネットワーク内に位置し前記通信データの宛先が前記第1の位置識別子により指定されているときには、前記処理手段は該通信データを該第1の位置識別子に対応する前記第3の位置識別子でカプセル化して、前記移動計算機のホームネットワークに設けられたデータパケット処理装置に送信することを特徴とする請求項13記載の中継装置。

【請求項17】 前記移動計算機が外部他組織ネットワ

4

ーク内に位置し前記通信データの宛先が前記第1の位置識別子により指定されているときには、前記処理手段は該通信データに含まれる該第1の位置識別子を対応する前記第2の位置識別子に置き換え、該通信データを前記第1の位置識別子に対応する前記第3の位置識別子でカプセル化して、前記外部他組織ネットワークに送信することを特徴とする請求項13記載の中継装置。

【請求項18】 複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能な通信ネットワークシステムで、該複数の計算機のうち少なくとも一つの計算機が通信ネットワークシステム上の位置を変更しながら通信を行う移動計算機である通信ネットワークシステムにおいて、前記移動計算機のホームネットワークに設けられて通信データを処理するデータパケット処理装置であって、

前記移動計算機に固有な該移動計算機の自組織ネットワーク内で一意に定められた第1の位置識別子と、該移動計算機に予約されたネットワーク全体で一意に定められた第2の位置識別子と、該移動計算機の通信ネットワークシステム上の現在の移動位置を示すネットワーク全体で一意に定められた第3の位置識別子と、の対応する組を含んだ前記移動計算機のアドレス情報を前記自組織ネットワーク内で管理する管理手段と、

前記移動計算機が外部他組織ネットワーク内に位置し前記通信データの宛先が前記第1の位置識別子により指定されているときには、ホームネットワーク内に設けられた中継装置から送信される前記第1の位置識別子に対応する前記第3の位置識別子でカプセル化された通信データを受け取り、前記第3の位置識別子によるカプセル化を解き、前記第3の位置識別子に対応する前記第2の位置識別子でカプセル化して、前記第3の位置識別子でカプセル化して、該外部他組織ネットワークに送信する処理手段と、を有することを特徴とするデータパケット処理装置。

【請求項19】 前記処理装置は前記通信データの暗号化/復号化処理も行うことを特徴とする請求項18記載のデータパケット処理装置。

【請求項20】 前記自組織ネットワークに属する移動計算機に予約された複数の位置識別子を管理し、前記外部他組織ネットワークに移動する各移動計算機に前記複数の位置識別子の一つを前記第2の位置識別子として貸し出す手段を有することを特徴とする請求項18記載のデータパケット処理装置。

【請求項21】 前記移動計算機が外部自組織ネットワーク内または前記外部他組織ネットワーク内に位置し前記通信データの宛先が前記第2の位置識別子により指定されているときには、前記処理手段は該第2の位置識別子を含む該通信データを該第2の位置識別子に対応する前記第3の位置識別子でカプセル化し、前記外部自組織ネットワークまたは前記外部他組織ネットワークに転送

することを特徴とする請求項1 8 記載のデータパケット処理装置。

【請求項2 2】 通信相手計算機が前記自組織ネットワーク外に位置し前記移動計算機が前記自組織ネットワーク内に位置するときには、前記処理手段は該移動計算機から送信される前記第1 の位置識別子をソースアドレスとした前記通信データを受け取り、前記第1 の位置識別子に対応する前記第2 の位置識別子をソースアドレスとするように整形して、前記通信相手計算機に送信することを特徴とする請求項1 8 記載のデータパケット処理装置。

【請求項2 3】 通信相手計算機が前記自組織ネットワーク内に位置し前記移動計算機が前記自組織ネットワーク外に位置するときには、前記処理装置は、前記第1 の位置識別子をソースアドレスとした前記通信データを作成した上で該第1 の位置識別子に対応する前記第2 の位置識別子でカプセル化して該移動計算機から送信された前記通信データを受け取り、カプセル化を解いて前記第2 の位置識別子を取り除いて、前記通信相手計算機に送信することを特徴とする請求項1 8 記載のデータパケット処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、相互接続している複数のネットワーク間で、相互にデータを交換し必要なサービスを提供する複数の計算機により構成されるシステムにおいて、それらの計算機のうちの一部がネットワークを渡って移動する場合に、それらの移動計算機へのアクセスを制御する通信制御方法に関する。

【0002】

【従来の技術】計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみならず、オフィス外あるいは一組織外とのコミュニケーション（例えば電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（Internet）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。

【0003】また、このようなネットワークの普及に伴い、移動通信（mobile computing）に

対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持ったユーザがネットワーク上を移動して通信する。ときには通信を行ないながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上のアドレスを管理し、正しく通信内容を到達させるための方式が必要である。

【0004】また、ネットワークが普及し、ネットワーク間の自由な接続が実現され、膨大なデータ、サービスのやりとりがなされる場合、セキュリティ上の問題を考慮する必要性が生じてくる。例えば、組織内部の秘密情報の外部ネットワークへの漏洩をいかに防ぐか、という問題や、組織外からの不正な侵入から、組織内ネットワークに接続された資源、情報をいかに守るか、という問題である。インターネットは、当初学術研究を目的に構築されたため、ネットワークの接続による自由なデータサービスのやりとりを重視しており、このようなセキュリティ上の問題は考慮されていなかったが、近年多くの企業、団体がインターネットに接続するようになり、セキュリティ上の問題から自組織ネットワークを防衛する機構が必要となってきた。

【0005】そこで、複数のネットワークを接続する際に、それらのネットワークを介して相互にやりとりされるデータを監視、チェックし、不正なアクセスが外部から侵入したり、内部データが外部に漏洩することを防止する機構を配置することが一般に行われている。このような機構をファイアウォールという。ファイアウォールを設置することにより、外部への秘密情報の漏洩、外部からの不正なアクセスを防ぎ、かつ内部から安全に外部のサービスを受けられるようになる。

【0006】また、特に機密性の高い重要データを外部ネットワークを介して通信する場合、外部にデータパケットを送出する前にその内容を暗号化し、受信したサイトで復号化する、という方法がある。この方法によれば、たとえ組織外のユーザが外部ネットワーク上のデータパケットを取り出しても、内容が暗号化されているので、決してその内容を漏洩することがなく、より安全な通信が確保できる。

【0007】このような暗号化通信をサポートするファイアウォールで守られた（ガードされた）ネットワーク通信であれば相互に暗号化通信が可能であるが、前述の移動計算機へのアクセスを考えると、その計算機が移動前に属していたネットワークと同じ組織に管理されるネットワーク内に移動し、かつその移動先ネットワークがファイアウォールにガードされているなら、あたかも同じネットワーク内の計算機同士で通信するように暗号化通信ができる。その場合のアドレス付けは組織内のプライベートアドレスを使用すれば十分である。

【0008】一方、移動計算機が外部組織のネットワーク、または自組織のネットワークであってもファイアウ

10

20

30

40

50

オールでガードされていないネットワークに移動した場合、その移動計算機は、外部の計算機として扱われなければならない。そのため暗号化通信はできないし、外部組織内では組織内のプライベートアドレスは使用できない(到達不能な場合がある)ので、全く別のアドレス付けが必要になる。

【0009】しかし、従来は、移動通信においては、移動計算機の現在の位置に応じてアドレスを付け変えるような処理は行っておらず、全てのネットワーク上で一意なアドレスを全ての移動計算機に与え、自組織内のアドレス(プライベートアドレス)と外部アドレスの対応表を管理して移動計算機にアクセスをしていた。

【0010】

【発明が解決しようとする課題】一部に外部ネットワーク(インターネット)で一意なアドレスの数は限られており、移動計算機が普及した場合、その各々に割り付けられるほどはない。しかるに今後ネットワーク上のセキュリティが問題視されるようになり、暗号化通信をサポートするようになると、移動計算機が移動前に属していたネットワークと同じ組織に管理されるネットワーク内に移動し、かつその移動先ネットワークが暗号化機構をサポートしているなら、あたかも同じネットワーク内の計算機同士で通信するように暗号化通信ができる。その場合のアドレス付けは組織内のプライベートアドレスを使用すれば十分であり、貴重な外部ネットワークアドレスを割り当てる必要もない。

【0011】しかし、移動計算機が外部組織のネットワークまたは自組織のネットワークであってもファイアウォールでガードされていないネットワークに移動した場合、その移動計算機は、外部の計算機として扱われなければならない、組織内のプライベートアドレスは使用できない。

【0012】そのために従来、移動通信においては、全てのネットワーク上で一意なアドレスを全ての移動計算機に与え、自組織内のアドレス(プライベートアドレス)と外部アドレスの対応表を管理して移動計算機にアクセスをしていた。

【0013】本発明は、上記事情を考慮してなされたものであり、複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能に構成された計算機システムで、移動計算機がネットワーク上の位置を変更しながら通信を行う場合に、移動計算機がネットワークのどのような位置に移動しても、柔軟なアドレス制御および管理が可能な通信制御方法、中継装置およびデータパケット処理装置を提供することを目的とする。

【0014】

【課題を解決するための手段】本発明は、複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能な通信ネットワークシステム

において、該複数の計算機のうち少なくとも一つの計算機が通信ネットワークシステム上の位置を変更しながら通信を行う移動計算機であるときの通信制御方法であって、(a)前記移動計算機がそのホームネットワーク内に位置するときには、該移動計算機に固有な該移動計算機の自組織ネットワーク内で一意に定められた第1の位置識別子により通信データを転送して該移動計算機に対する通信を行い、(b)前記移動計算機が外部自組織ネットワーク内に位置するときには、該移動計算機の通信ネットワークシステム上の現在の移動位置を示すネットワーク全体で一意に定められた第3の位置識別子により通信データを該外部自組織ネットワークにルーティングし、該外部自組織ネットワーク内では前記第1の位置識別子により該移動計算機をアドレッシングして該移動計算機に対する通信を行い、(c)前記移動計算機が外部他組織ネットワーク内に位置するときには、前記第3の位置識別子により通信データを該外部他組織ネットワークにルーティングし、該外部他組織ネットワーク内では該移動計算機が自組織外に移動する際に該移動計算機に貸し与えられるネットワーク全体で一意に定められた第2の位置識別子により該移動計算機をアドレッシングして該移動計算機に対する通信を行う、ことを特徴とする。

【0015】また、本発明は、上記通信制御方法において、互いに対応する前記第1の位置識別子、前記第2の位置識別子、前記第3の位置識別子の組を含んだ前記移動計算機のアドレス情報を前記自組織ネットワーク内で管理することを特徴とする。

【0016】また、本発明は、上記通信制御方法において、通信相手計算機が前記自組織ネットワーク内に位置するときには、該通信相手計算機から通信データを前記移動計算機の前記第1の位置識別子を付けて送信し、前記移動計算機が前記外部自組織ネットワーク内または前記外部他組織ネットワーク内に位置するときには、前記ホームネットワーク内に設けられた中継装置において前記通信データに付けられた前記第1の位置識別子に対応する前記第3の位置識別子を前記アドレス情報に基づいて求め、該通信データに該第3の位置識別子を付けて該中継装置から該移動計算機の現在の移動位置へ転送する、ことを特徴とする。

【0017】また、本発明は、上記通信制御方法において、通信相手計算機が前記自組織ネットワーク外に位置するときには、該通信相手計算機から通信データを前記移動計算機の前記第2の位置識別子を付けて送信し、前記移動計算機が前記外部自組織ネットワーク内または前記外部他組織ネットワーク内に位置するときには、前記ホームネットワーク内に設けられたデータパケット処理装置において前記通信データに付けられた前記第2の位置識別子に対応する前記第3の位置識別子を前記アドレス情報に基づいて求め、該通信データに該第3の位置識別子を付けて該データパケット処理装置から該移動計算

10

20

30

40

50

機の現在の移動位置へ転送する、ことを特徴とする。

【0018】また、本発明は、上記通信制御方法において、前記管理するステップは、前記アドレス情報を前記ホームネットワーク内に設けられた中継装置において管理することを特徴とする。

【0019】また、本発明は、上記通信制御方法において、前記管理するステップは、前記アドレス情報を前記ホームネットワーク内に設けられたデータパケット処理装置において管理することを特徴とする。

【0020】また、本発明は、上記通信制御方法において、前記管理するステップは、前記アドレス情報を前記ホームネットワーク外に設けられた外部中継装置において管理し、前記移動計算機の位置登録処理の際に該アドレス情報を更新することを特徴とする。

【0021】また、本発明は、上記通信制御方法において、前記管理するステップは、前記アドレス情報を前記自組織ネットワークに設けられたデータベースにおいて管理し、該データベースは該自組織ネットワークに属する計算機のアドレス情報を記憶して要求に応じて要求されたアドレス情報を返すことを特徴とする。

【0022】また、本発明は、上記通信制御方法において、前記管理するステップは、前記移動計算機が前記自組織ネットワーク外に移動するにあたって前記第2の位置識別子を獲得したときに前記アドレス情報を更新することを特徴とする。

【0023】また、本発明は、上記通信制御方法において、前記管理するステップは、前記アドレス情報に対応してバージョン番号を管理し、前記移動計算機の結果該アドレス情報が更新されたときに該バージョン番号を更新することを特徴とする。

【0024】また、本発明は、上記通信制御方法において、前記管理するステップは、前記アドレス情報に対応してアドレス情報の有効期限を管理し、該有効期限が過ぎたときに該アドレス情報を無効化することを特徴とする。

【0025】また、本発明は、上記通信制御方法において、前記管理するステップは、前記移動計算機から該移動計算機の最登録を要求するメッセージを受け取ったときに前記有効期限を初期化すること、特徴とする。

【0026】また、本発明は、上記通信制御方法において、前記管理するステップは、新たな移動位置に移動した前記移動計算機から新たな第3の位置識別子の登録を要求するメッセージを受け取り、該メッセージに含まれた署名情報にもとづいて該移動計算機が正しく認証されたときに、前記アドレス情報の前記第3の位置識別子を書き換えることを特徴とする。

【0027】また、本発明は、上記通信制御方法において、前記管理するステップは、前記移動計算機から該移動計算機の切断を要求するメッセージを受け取ったときに前記アドレス情報を無効化し、該アドレス情報の無

効化を該移動計算機に通知することを特徴とする。

【0028】また、本発明は、上記通信制御方法において、前記第3の位置識別子は、前記移動計算機が移動先ネットワークで獲得したネットワーク全体で一意に定められた位置識別子であることを特徴とする。

【0029】また、本発明は、上記通信制御方法において、前記第3の位置識別子は、前記ホームネットワーク外に移動した前記移動計算機を直接管理し、該移動計算機と通信相手計算機との間の通信データを中継する外部中継装置を示し、ネットワーク全体で一意に定められた位置識別子であることを特徴とする。

【0030】また、本発明は、上記通信制御方法において、前記外部中継装置は、前記第3の位置識別子に基づいて転送された通信データを受け取り、該通信データに付けられた前記第1の位置識別子または前記第2の位置識別子に基づいて該通信データを前記移動計算機に送ることを特徴とする。

【0031】また、本発明は、上記通信制御方法において、前記第2の位置識別子は、前記ホームネットワーク内の中継装置により予約された複数の位置識別子から、前記移動計算機が外部他組織ネットワークに移動する際に該移動計算機に貸し与えられることを特徴とする。

【0032】また、本発明は、上記通信制御方法において、前記第2の位置識別子は、前記ホームネットワーク内のデータパケット処理装置により予約された複数の位置識別子から、前記移動計算機が外部他組織ネットワークに移動する際に該移動計算機に貸し与えられることを特徴とする。

【0033】また、本発明は、上記通信制御方法において、前記第2の位置識別子は、前記ホームネットワーク外の外部中継装置により予約された複数の位置識別子から、前記移動計算機が外部他組織ネットワークに移動したときに該移動計算機に貸し与えられることを特徴とする。

【0034】また、本発明は、上記通信制御方法において、前記ステップ(b)において、前記通信データの宛先が前記第1の位置識別子により指定されているときには、該第1の位置識別子を含む該通信データを該第1の位置識別子に対応する前記第3の位置識別子でカプセル化し、前記外部自組織ネットワークに転送することを特徴とする。

【0035】また、本発明は、上記通信制御方法において、前記ステップ(b)および(c)において、前記通信データの宛先が前記第2の位置識別子により指定されているときには、該第2の位置識別子を含む該通信データを該第2の位置識別子に対応する前記第3の位置識別子でカプセル化し、前記外部自組織ネットワークまたは前記外部他組織ネットワークに転送することを特徴とする。

【0036】また、本発明は、上記通信制御方法におい

て、前記通信データは、暗号化しないカプセル化によりカプセル化することを特徴とする。

【 0 0 3 7 】また、本発明は、上記通信制御方法において、前記ステップ(c)において、前記通信データの宛先が前記第1 の位置識別子により指定されているときには、前記ホームネットワーク内に設けられた中継装置が、該通信データを該第1 の位置識別子に対応する前記第3 の位置識別子でカプセル化して送信し、前記ホームネットワーク内に設けられたデータパケット処理装置が、前記中継装置から送信された通信データを受け取り、該第3 の位置識別子によるカプセル化を解き、該第3 の位置識別子に対応する前記第2 の位置識別子でカプセル化し、該第3 の位置識別子でカプセル化して、前記外部他組織ネットワークに送信することを特徴とする。

【 0 0 3 8 】また、本発明は、上記通信制御方法において、前記ステップ(c)において、前記通信データの宛先が前記第1 の位置識別子により指定されているときには、前記ホームネットワーク内に設けられた中継装置が、該通信データに含まれる該第1 の位置識別子に対応する前記第2 の位置識別子に置き換え、該通信データを該第1 の位置識別子に対応する前記第3 の位置識別子でカプセル化して、前記外部他組織ネットワークに送信することを特徴とする。

【 0 0 3 9 】また、本発明は、上記通信制御方法において、前記ステップ(c)において、前記ホームネットワーク外に設けられた外部中継装置が通信データを受け取り、前記第3 の位置識別子によるカプセル化を解いて、該通信データに含まれる前記第2 の位置識別子を使って前記移動計算機に転送することを特徴とする。

【 0 0 4 0 】また、本発明は、上記通信制御方法において、通信相手計算機が前記自組織ネットワーク内に位置するときには、該通信相手計算機から前記第1 の位置識別子を付けて前記通信データを送信し、前記通信相手計算機が前記自組織ネットワーク外に位置するときには、該通信相手計算機から前記第2 の位置識別子を付けて前記通信データを送信することを特徴とする。

【 0 0 4 1 】また、本発明は、上記通信制御方法において、前記通信移動計算機が前記自組織ネットワーク内に位置するときには、該移動計算機から前記第1 の位置識別子をソースアドレスとして前記通信データを送信し、前記移動計算機が前記自組織ネットワーク外に位置するときには、該移動計算機から前記第2 の位置識別子をソースアドレスとして前記通信データを送信することを特徴とする。

【 0 0 4 2 】また、本発明は、上記通信制御方法において、通信相手計算機が前記自組織ネットワーク外に位置し前記移動計算機が前記自組織ネットワーク内に位置するときには、該移動計算機から前記第1 の位置識別子をソースアドレスとして前記通信データを送信し、前記ホームネットワークに設けられたデータパケット処理装置

において、前記移動計算機が送信された前記通信データを受け取り、ソースアドレスを前記第1 の位置識別子から前記第1 の位置識別子に対応する前記第2 の位置識別子に置き換えて、前記通信相手計算機に送信することを特徴とする。

【 0 0 4 3 】また、本発明は、上記通信制御方法において、通信相手計算機が前記自組織ネットワーク内に位置し前記移動計算機が前記自組織ネットワーク外に位置するときには、該移動計算機において、前記第1 の位置識別子をソースアドレスとした前記通信データを作成し、該第1 の位置識別子に対応する前記第2 の位置識別子でカプセル化して送信し、前記ホームネットワークに設けられたデータパケット処理装置において、前記移動計算機から送信された前記通信データを受け取り、カプセル化を解いて前記第2 の位置識別子を取り除いて、前記通信相手計算機に送信することを特徴とする。

【 0 0 4 4 】さらに、本発明は、複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能な通信ネットワークシステムで、該複数の計算機のうち少なくとも一つの計算機が通信ネットワークシステム上の位置を変更しながら通信を行う移動計算機である通信ネットワークシステムにおいて、前記移動計算機のホームネットワークに設けられて通信データを中継する中継装置であって、前記移動計算機に固有な該移動計算機の自組織ネットワーク内で一意に定められた第1 の位置識別子と、該移動計算機に予約されたネットワーク全体で一意に定められた第2 の位置識別子と、該移動計算機の通信ネットワークシステム上の現在の移動位置を示すネットワーク全体で一意に定められた第3 の位置識別子と、の対応する組を含んだ前記移動計算機のアドレス情報を前記自組織ネットワーク内で管理する管理手段と、送信元計算機から送信された通信データに付加された前記第1 の位置識別子または前記第2 の位置識別子に対応する前記第3 の位置識別子を前記アドレス情報から求め、得られた前記第3 の位置識別子を前記通信データに付加して前記宛先計算機に向けて転送する処理手段と、を有することを特徴とする。

【 0 0 4 5 】また、本発明は、上記中継装置において、前記自組織ネットワークに属する移動計算機に予約された複数の位置識別子を管理し、外部他組織ネットワークに移動する各移動計算機に前記複数の位置識別子の一つを前記第2 の位置識別子として貸し出す手段を有することを特徴とする。

【 0 0 4 6 】また、本発明は、上記中継装置において、前記移動計算機が外部自組織ネットワーク内に位置し前記通信データの宛先が前記第1 の位置識別子により指定されているときには、前記処理手段は該第1 の位置識別子を含む該通信データを該第1 の位置識別子に対応する前記第3 の位置識別子でカプセル化し、前記外部自組織ネットワークに転送することを特徴とする。

10

20

30

40

50

13

【 0 0 4 7 】また、本発明は、上記中継装置において、前記移動計算機が外部他組織ネットワーク内に位置し前記通信データの宛先が前記第1 の位置識別子により指定されているときには、前記処理手段は該通信データを該第1 の位置識別子に対応する前記第3 の位置識別子でカプセル化し、前記移動計算機のホームネットワークに設けられたデータパケット処理装置に送信することを特徴とする。

【 0 0 4 8 】また、本発明は、上記中継装置において、前記移動計算機が外部他組織ネットワーク内に位置し前記通信データの宛先が前記第1 の位置識別子により指定されているときには、前記処理手段は該通信データに含まれる該第1 の位置識別子に対応する前記第2 の位置識別子に置き換え、該通信データを前記第1 の位置識別子に対応する前記第3 の位置識別子でカプセル化して、前記外部他組織ネットワークに送信することを特徴とする。

【 0 0 4 9 】さらに、本発明は、複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能な通信ネットワークシステムで、該複数の計算機のうち少なくとも一つの計算機が通信ネットワークシステム上の位置を変更しながら通信を行う移動計算機である通信ネットワークシステムにおいて、前記移動計算機のホームネットワークに設けられて通信データを処理するデータパケット処理装置であって、前記移動計算機に固有な該移動計算機の自組織ネットワーク内で一意に定められた第1 の位置識別子と、該移動計算機に予約されたネットワーク全体で一意に定められた第2 の位置識別子と、該移動計算機の通信ネットワークシステム上の現在の移動位置を示すネットワーク全体で一意に定められた第3 の位置識別子と、の対応する組を含んだ前記移動計算機のアドレス情報を前記自組織ネットワーク内で管理する管理手段と、前記移動計算機が外部他組織ネットワーク内に位置し前記通信データの宛先が前記第1 の位置識別子により指定されているときには、前記ホームネットワーク内に設けられた中継装置から送信される前記第1 の位置識別子に対応する前記第3 の位置識別子でカプセル化された通信データを受け取り、前記第3 の位置識別子によるカプセル化を解き、前記第3 の位置識別子に対応する前記第2 の位置識別子でカプセル化し、前記第3 の位置識別子でカプセル化して、該外部他組織ネットワークに送信する処理手段と、有することを特徴とする。

【 0 0 5 0 】また、本発明は、上記データパケット処理装置において、前記処理装置は前記通信データの暗号化／復号化処理も行うことを特徴とする。

【 0 0 5 1 】また、本発明は、上記データパケット処理装置において、前記自組織ネットワークに属する移動計算機に予約された複数の位置識別子を管理し、前記外部他組織ネットワークに移動する各移動計算機に前記複数

14

の位置識別子の一つを前記第2 の位置識別子として貸し出す手段を有することを特徴とする。

【 0 0 5 2 】また、本発明は、上記データパケット処理装置において、前記移動計算機が外部自組織ネットワーク内または前記外部他組織ネットワーク内に位置し前記通信データの宛先が前記第2 の位置識別子により指定されているときには、前記処理手段は該第2 の位置識別子を含む該通信データを該第2 の位置識別子に対応する前記第3 の位置識別子でカプセル化し、前記外部自組織ネットワークまたは前記外部他組織ネットワークに転送することを特徴とする。

【 0 0 5 3 】また、本発明は、上記データパケット処理装置において、通信相手計算機が前記自組織ネットワーク外に位置し前記移動計算機が前記自組織ネットワーク内に位置するときには、前記処理手段は該移動計算機から送信される前記第1 の位置識別子をソースアドレスとした前記通信データを受け取り、前記第1 の位置識別子に対応する前記第2 の位置識別子をソースアドレスとするように整形して、前記通信相手計算機に送信することを特徴とする。

【 0 0 5 4 】また、本発明は、上記データパケット処理装置において、通信相手計算機が前記自組織ネットワーク内に位置し前記移動計算機が前記自組織ネットワーク外に位置するときには、前記処理装置は、前記第1 の位置識別子をソースアドレスとした前記通信データを作成した上で該第1 の位置識別子に対応する前記第2 の位置識別子でカプセル化して該移動計算機から送信された前記通信データを受け取り、カプセル化を解いて前記第2 の位置識別子を取り除いて、前記通信相手計算機に送信することを特徴とする。

【 0 0 5 5 】本発明によれば、移動計算機がネットワーク間を移動する場合、移動計算機の情報が更新される場合、移動計算機の情報が無効化される場合など様々な制御情報に対応可能であり、その結果様々な移動プロトコルにも柔軟に対応可能な移動通信環境を提供できる。

【 0 0 5 6 】

【 発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【 0 0 5 7 】図1 に、本実施形態に係るネットワークの基本構成を示す。本実施形態では、自組織ネットワーク1 a、外部の自組織ネットワーク1 b および外部組織ネットワーク1 c が外部ネットワーク1 d を介して相互に接続されており、自組織ネットワーク1 a をホームとする移動ホスト計算機2 1 がネットワーク1 b、1 c に移動する場合を考える。自組織ネットワーク1 a、1 bにはそれらが管理する計算機間でデータ内容を(暗号化などにより)秘匿して通信を行うためのデータパケット処理装置3 a、3 b が設置されており、自組織の管理するホスト間での秘匿通信を達成する。

【 0 0 5 8 】図2 は、本実施形態に係る通信制御方法に

50

における3種類の位置識別子を記憶する位置識別子記憶部の一構成例を示す。この位置識別子記憶部は具体的には3つのアドレスを連結したテーブルとして実現される。ここで、H-a d d r (h o m e a d d r e s s) は移動ホスト 計算機21に固有の自組織のネットワーク内で一意に定められたアドレスを示し、M-a d d r (m o b i l e a d d r e s s) は移動ホスト 計算機21に予約されたネットワーク全体で一意に定められたアドレスを示し、C-a d d r (C a r e - o f a d d r e s s) は移動ホスト 計算機21がネットワーク上で移動した現在地を示すネットワーク全体で一意に定められたアドレスを示す。また、このテーブルには後述するように移動通信プロトコルで定められたその他の情報群を連結して格納することが可能である。

【0059】3つの位置識別子を含むテーブルは、システムの構成に応じて、例えば、ネットワーク上のあるホスト上、ゲートウェイ上、ルータ上など、様々な場所に置くことが可能である。本実施形態では、各データパケット処理装置3a, 3b内にその3つの位置識別子を含むテーブルを持つものとする。

【0060】さて、一般に1つの組織に与えられるインターネット上で一意なIPアドレス(インターネットアドレス)の数には限りがある。しかし各組織とも多くのホストをサポートする必要があるため、外部とデータをやりとりするゲートウェイ計算機にのみインターネットアドレスを割り当てて、それ以外のアドレスにはその組織内で独自に定めるプライベートアドレスを割り当てることが通常行われる。

【0061】図1のネットワーク構成では、自組織ネットワーク1a, 1b内の全ての計算機は自組織のプライベートアドレスを割り当てられている。本来の位置で接続されている計算機2だけでなく、移動ホスト 計算機21についても移動前には自組織ネットワーク1a内でのプライベートアドレスが割り当てられていた。このプライベートアドレスが3つ組アドレスのうちH-a d d r (h o m e a d d r e s s) に対応する。自組織内のホストは全てプライベートアドレスを持っているので、移動ホスト 計算機21がネットワーク1bに移動しても、ネットワーク1bの全ネットワーク内での位置を示すアドレス(これがC-a d d r (c a r e - o f a d d r e s s) に相当する)を用いて、そのネットワーク内に入ることができれば、あとはプライベートアドレス(H-a d d r)によるアドレッシングが可能である。

【0062】一方、もし、移動ホスト 計算機21が外部組織ネットワーク1c内に移動した場合、自組織内のプライベートアドレスは外部組織では使用できないため、ネットワーク1c内にいる移動ホスト 計算機21に対しルーティングできない。そのような場合に使用するのがM-a d d r (m o b i l e a d d r e s s) である。M-a d d r は移動ホスト 群(移動ホスト 計算機2

1を含む)のために予約されたインターネットアドレスである。従って、M-a d d r を使用すれば移動ホスト 計算機21が外部組織ネットワーク1c上に移動しても、インターネット全体で一意にルーティングが可能である。

【0063】以上のように、移動ホスト 計算機21と通信を行う場合、その移動ホスト 計算機21の現在位置と使用する移動通信プロトコルに応じて、格納された3つのアドレスを適宜切替えて使用する。

【0064】すなわち、本実施形態に係る通信制御方法による移動通信の制御の原則は、外部組織ネットワーク内の移動ホストと通信を行う場合はC-a d d r を使って外部組織ネットワークにルーティングし、その中ではM-a d d r で移動ホストにアドレッシングし、外部の自組織ネットワークにいる移動ホストと通信を行う場合はC-a d d r を使って外部の自組織ネットワークにルーティングし、その中ではH-a d d r で移動ホストにアドレッシングし、内部ネット内の移動ホストと通信を行う場合はH-a d d r 宛にデータパケットを送るよう制御する。この原則を既に提案されている様々な移動通信プロトコルに対して、適宜規則を追加して実際の運用に適用する。

【0065】以下では、現在提案されている主要な移動通信プロトコルであるIETF/Mobile-IP(参考文献: C. Perkins (IBM): "IP Mobility Support (draft-ietf-mobileip-protocol-12.txt)", Internet Draft, 1995/8.)とVIP(参考文献: Teraoka F. et al. "VIP: A Protocol Providing Host Mobility, CACM Vol. 37, No. 8, pp. 67-75 (Aug. 1994)")を例にとり、本発明を用いて各移動通信プロトコルがどのように実装されるかを示す。

【0066】まず、IETF/mobile-IPの実装例について説明する。

【0067】IETF/Mobile-IP(以下MIPと略記する)は、図3に示すように移動ホストMH、外部エージェントFA(図中の36)、ホームエージェントHA(図中35)、通信相手CHから構成される。なお、図3では、各ネットワーク31, 32, 33, 34を相互接続する外部ネットワークは省略してある。外部エージェントFAは自らの管理する範囲に移動した移動ホストMHを管理している。通信相手CHから送信された、それらの移動ホストHM宛のデータは、一旦ホームエージェントHAに送られる。その後、外部エージェントFAを経由して転送先の移動ホストMHに送られる(図中37)。

【0068】また、MIPでは、上記のように外部エージェントFAを使って通信するFA使用モード(図3の

17

MH2)の他に、移動ホストMHがネットワークレイヤのインターネットアドレスを得た上で(例えば文献: R. Droms: "Dynamic Host Configuration Protocol", IETF-RFC1541, Oct. 1993に示された方式)通信を行うpop-upモードと呼ばれるモード(図3のMH1)が指定されている。

【0069】本発明をMIPに適用する際の、位置識別子記憶部の構成例を図4に示す。

【0070】MIPでは、各移動ホストMHに対する登録情報にはlifetime(情報の有効期限)を付加して管理する。ここでは、前述の位置識別子記憶部にlifetimeを示すフィールドを付けてこの管理を行う。

【0071】本発明に係る通信制御方法をMIPに適用する場合は、ホームエージェントHA内と各外部エージェントFA内(FAモードの場合)に、lifetimeを含むH-addrとC-addrの対応表を設けるとともに、ネットワーク上のデータパケット処理装置(図1の3a, 3b)に図4に示すような位置識別子記憶部を設ける。これらを用いてMIPの制御、実際の移動ホストへの通信制御を行う。

【0072】以下、FA使用モード、pop-upモードの2通りの場合について、MIPの各動作を説明する。

【0073】(1)MIPの登録

ホームの自組織ネットワーク外に移動したホストMHは、登録を行なうために、「登録要求」メッセージをホームエージェントHAに出す。

【0074】FA使用モードでは、「登録要求」メッセージは、メッセージ内のC-addr部に外部エージェントFAのアドレスを付け、外部エージェントFA経由で送られる。

【0075】pop-upモードでは、メッセージ内のC-addr部は、移動ホストMHが移動先ネットワークで獲得したインターネットアドレスとする。

【0076】「登録要求」メッセージを受けたホームエージェントHAは、要求を受け付けることができる場合、「確認」の応答を移動ホストMHに返す。例えば、移動ホストMHにより付されたメッセージ内の署名情報を調べて転送元計算機を認証し、認証が正しく行われた場合に新たに登録する。

【0077】要求を受け付けることができない場合、認証が正しく行われなかったときの「認証失敗」の応答あるいはその他の理由に応じた「無効」や「登録拒否」の応答を移動ホストMHに返す。「確認」の応答の場合は、ホームエージェントHA内のテーブルに3つ組アドレスが登録される。なお、FA使用モードでは、外部エージェントFAも3つ組アドレスを保持、管理する。

【0078】(2)MIPのkeep-alive

18

移動ホストMHは、ホームエージェントHA、外部エージェントFAの広告に書かれるlifetimeより短い周期で、keep-aliveと呼ばれる再登録を行う。

【0079】再登録によりホームエージェントHA、外部エージェントFAに登録されていた3つ組アドレス情報のlifetime値が初期値に戻る。

【0080】(3)MIPの切断

移動ホストMHは、切断を行なう場合、ホームエージェントHAに直接、切断要求メッセージを送る。

【0081】ホームエージェントHAは、移動ホストMHに切断リクエストの成功/失敗を送信するとともに、対応する3つ組アドレスを無効とする。

【0082】FA使用モードの場合、外部エージェントFAには何もメッセージは送られないが、lifetimeにより自動的に無効化される。ただし、システム要求によっては、ホームエージェントHAから外部エージェントFAにメッセージを送るようにしても構わない。

【0083】(4)MIPの移動

上記(1)の登録が済んでいる移動ホストMHは、さらに移動した場合、適当な間隔で上記(2)のkeep-aliveにより再登録を行う。

【0084】FA使用モードでは、移動により移動ホストMHを管理する外部エージェントFAが替わった場合、keep-aliveメッセージに伴い、新たなFAアドレスがメッセージのC-addr部に書き込まれる。以降、通信は再登録された3つ組アドレスにより継続可能である。

【0085】なお、pop-upモードでは同一サブネットワーク内の移動でアドレスが変化しない場合は再登録の手続きは不要である。ただし、pop-upモードでアドレスを再取得して変更した場合の動作は、FA使用モードでFAが変わった場合と同様である。

【0086】(5)MIPのデータ通信

次に、MIPのデータ通信の方法について説明する。原則として、移動ホストMHへのアドレッシングは、プライベートアドレスを共有する同一組織内ではH-addrで行い、それ以外の外部組織にある移動ホストMHに対してはM-addrで行う。

【0087】最初に、FA使用モードの場合について説明する。

【0088】図5はFA使用モードのネットワーク構成の一例である。自組織ネットワーク41は、移動ホストMHが本来接続されていたホームネットワークである。外部の自組織ネットワーク42は、自組織ネットワーク41と同じ組織に管理されており、互いに共通のプライベートアドレス(すなわちH-addr)で各ホストを一意にアドレッシング可能であるとする。ネットワーク43, 44は、外部組織のネットワークである。また、ネットワーク41の出口と移動ホストMHに附属してデー

タパケット処理装置45, 46が設置されており、秘匿通信(暗号化通信)をサポートするものとする。なお、図5中では、FA使用モードで自組織ネットワーク41内のFAの機能を有する装置を省略してある。

【0089】FA使用モードでは、移動ホストMHから通信相手CHに向かう通信は直接、通信相手CH宛にルーティングされる。また、通信相手CHから移動ホストMHへの通信はホームエージェントHAに送られた後、その時点で移動ホストMHを管理する外部エージェントFAに転送され、その外部エージェントFAから移動ホストMHに送られる。

【0090】FA使用モードにおける動作を通信相手CH、移動ホストMHの位置関係によって場合分けし、図6～図8の動作フローチャートを参照しながら説明する。

【0091】通信相手CHと移動ホストMHの位置関係は、次の10のケースが考えられる。

【0092】case 1は、通信相手CHの位置がネットワーク41内で、移動ホストMHの位置がネットワーク41の場合である。

【0093】case 2は、通信相手CHの位置がネットワーク41内で、移動ホストMHの位置がネットワーク42の場合である。

【0094】case 3は、通信相手CHの位置がネットワーク41内で、移動ホストMHの位置がネットワーク43の場合である。

【0095】case 4は、通信相手CHの位置がネットワーク42内で、移動ホストMHの位置がネットワーク41の場合である。

【0096】case 5は、通信相手CHの位置がネットワーク42内で、移動ホストMHの位置がネットワーク42の場合である。

【0097】case 6は、通信相手CHの位置がネットワーク42内で、移動ホストMHの位置がネットワーク43の場合である。

【0098】case 7は、通信相手CHの位置がネットワーク43内で、移動ホストMHの位置がネットワーク41の場合である。

【0099】case 8は、通信相手CHの位置がネットワーク43内で、移動ホストMHの位置がネットワーク42の場合である。

【0100】case 9は、通信相手CHの位置がネットワーク43内で、移動ホストMHの位置がネットワーク43の場合である。

【0101】case 10は、通信相手CHの位置がネットワーク43内で、移動ホストMHの位置がネットワーク44の場合である。

【0102】図6は、上記のcase 1, case 2, case 4, case 5の場合の動作である。

【0103】図7は、上記のcase 3, case 6の

場合の動作である。

【0104】図8は、上記のcase 7～case 10の場合の動作である。

【0105】(case 1, case 2) case 1とcase 2では、通信相手CHは、データパケットに移動ホストMHのH-a d d r を付けて送出する。その結果、パケットはホームエージェントHAに到達する。この移動ホストMHのH-a d d r を付けたデータを受信すると(ステップS 1 1)、もし秘匿通信が必要なら(ステップS 1 2 YES)、データパケット処理装置45がこのパケットのペイロードを暗号化する(ステップS 1 3)。そして、暗号化する場合にはデータパケット処理装置45によりステップS 1 4で、また暗号化しない場合にはホームエージェントHAによりステップS 1 5で、このパケットは移動ホストMHのH-a d d r に対応するC-a d d r (移動ホストMHが位置するネットワーク内のFAアドレス)でカプセル化されて送出される。その結果、パケットは外部エージェントFAに転送される。外部エージェントFAでは、カプセル化を解き、中のアドレス(H-a d d r)で移動ホストMHに転送する(ステップS 1 6)。

【0106】ここで、両者が秘匿通信を行う場合は、データパケット処理装置45が暗号化処理を行う。ただし、FAは暗号を解読できないので、ステップS 1 4のC-a d d r を付けるカプセル化としては、後述する「暗号化しないカプセル化」を行う。

【0107】なお、case 1の場合、移動ホストMHと通信相手CHが同一リンクにあるなら、両者ともH-a d d r を使って直接通信することができる。

【0108】(case 3) case 3では、通信相手CHはデータパケットに移動ホストMHのH-a d d r を付けて送出する。その結果、パケットはホームエージェントHAに到達する。この移動ホストMHのH-a d d r を付けたデータを受信すると(ステップS 2 1)、ホームエージェントHAは、移動ホストMHのH-a d d r に対応するC-a d d r (ネットワーク43内のFAアドレス)でカプセル化し、送出する(ステップS 2 2)。その結果、パケットはFAに向けて送り出される。ここで、転送途中のデータパケット処理装置45にて、FA経由のMIPであることを検出した場合、C-a d d r によるカプセル化を解き、C-a d d r に対応するM-a d d r を検索し、このM-a d d r でカプセル化し、さらにC-a d d r でカプセル化して送出する(ステップS 2 3)。FAはカプセル化を解き、中のM-a d d r で移動計算機MHに転送する(ステップS 2 4)。(ネットワーク43は組織外部なのでH-a d d r が使えない。)ここで、両者が秘匿通信を行う場合は、データパケット処理装置45にてM-a d d r でカプセル化のときに暗号化する。

【0109】また、次のような手順をとることもでき

る。

【0110】通信相手CHはデータパケットに移動ホストMHのH-a d d r を付けて送出する。その結果、パケットはホームエージェントHAに到達する。この移動ホストMHのH-a d d r を付けたデータを受けたホームエージェントHAは、移動ホストMHのH-a d d r をこれに対応するM-a d d r に置き換えた後、対応するC-a d d r (ネットワーク43内のFAアドレス) でカプセル化し、送出する。その結果、パケットはFAに転送される。FAはカプセル化を解き、中のM-a d d r で移動ホストMHに転送する。

【0111】ここで、両者が秘匿通信を行う場合は、データパケット処理装置45が暗号化処理を行う。ただし、FAは暗号を解読できないので、C-a d d r を付けるカプセル化としては、後述する「暗号化しないカプセル化」を行う。

【0112】(case 4) case 4 では、case 2と同様の処理を行う。ネットワーク42にデータパケット処理装置が設置されていれば、秘匿通信もcase 2と同様に可能である。

【0113】(case 5) case 5 では、case 2と同様の処理を行う。

【0114】(case 6) case 6 では、case 3と同様の処理を行う。ネットワーク42にデータパケット処理装置が設置されていれば、秘匿通信もcase 3と同様に可能である。

【0115】(case 7 ~ case 10) case 7 ~ case 10 では、通信相手CHがデータパケット処理装置の設置されていないネットワーク43にあるので、秘匿通信は行わないものとする。また、通信相手CHは、組織外部のネットワークにいたので、通信相手CHは移動ホストMHのH-a d d r を知らない点が前述のケースと異なっている。

【0116】case 7 ~ case 10 では、通信相手CHはパケットに移動ホストMHのM-a d d r を付けて送出する。その結果、パケットはネットワーク41のデータパケット処理装置45に到達する。この移動ホストMHのM-a d d r を付けたデータを受信すると(ステップS31)、データパケット処理装置45は移動ホストMHの3つ組アドレスを検索し、対応するC-a d d r でカプセル化して送出する(ステップS32)。その結果、パケットはFAに転送される。FAはカプセル化を解き、中のM-a d d r で移動ホストMHに転送する(ステップS33)。

【0117】なお、case 7 では、データパケット処理装置45と移動ホストMHが同一のリンクにある場合は、移動ホストMHのC-a d d r をH-a d d r と同一に登録しておき、これを検出したら、カプセル化およびFAへの転送をせず、直接転送するようにすることもできる。

【0118】以上はCHがHAを経由してMH宛にデータを転送する場合の処理を示したが、逆方向のMH発CH宛のデータ転送についても、CHがどのようにアドレス付けられているかに応じて、MH発パケットのソースアドレスをH-a d d r またはM-a d d r に付け換えることが必要である。

【0119】まず、CHが外部ネットワークである場合(case 7 ~ case 10)、MHはソースアドレスとして自身のM-a d d r を使用する。これは例えば応答メッセージなどを返信される場合に、グローバルであるM-a d d r を使用しないとルーティングができないからである。

【0120】但し、MHがプライベートアドレス領域にいる場合(case 7 ~ case 8) には、M-a d d r をつけたパケットは自組織内では使用できないので、H-a d d r をソースにして、データパケット処理装置まで到達させ、そこでH-a d d r を該当するM-a d d r に置き換えて、さらにデータが送信される。

【0121】一方、CHがプライベートアドレス領域にいて、MHが外部ネットワークにいる場合(case 3, case 6) には、H-a d d r をソースアドレスにしたパケットを、M-a d d r でカプセル化して送信し、CHのいるネットワークのデータパケット処理装置まで到達させて、そこで外側のM-a d d r 部分のカプセル化を解いてCHに転送する。

【0122】次に、pop-up モードにおける通信手順を、前述した各CASEについて、図9、図10の動作フローチャートを参照しながら説明する。

【0123】図9は、case 1 ~ case 6 の場合のデータパケット処理装置の動作である。

【0124】図10は、case 7 ~ case 10 の場合のデータパケット処理装置の動作である。

【0125】pop-up モードの場合、FAが存在せず、移動ホストMHが自身のインターネットアドレスを獲得するので、3つ組アドレス情報を登録する際に、獲得したインターネットアドレスをC-a d d r として登録する。

【0126】(case 1 ~ case 3) case 1 ~ case 3 では、通信相手CHは、データパケットに移動ホストMHのH-a d d r を付けて送出する。その結果、パケットはホームエージェントHAに到達する。この移動ホストMHのH-a d d r を付けたデータを受信すると(ステップS41)、もし秘匿通信が必要なら(ステップS42 YES)、データパケット処理装置45がこのパケットのペイロードを暗号化する(ステップS43)。そして、暗号化する場合にはデータパケット処理装置45によりステップS44で、また暗号化しない場合にはホームエージェントHAによりステップS45で、このパケットは移動ホストMHのH-a d d r に対応するC-a d d r (移動ホストMHのアドレス) で

カプセル化されて送出される。その結果、パケットは移動ホストMHに転送される。ここで、秘匿通信を行う場合のC-a d d r を付けるカプセル化としては、後述する「暗号化しないカプセル化」を行う。

【0127】ここで、両者が秘匿通信を行う場合は、ステップS43とS44においてデータパケット処理装置45で一旦C-a d d r のカプセル化を解き、暗号化の後、再度C-a d d r でカプセル化して送出する。

【0128】なお、case1の場合、移動ホストMHと通信相手CHが同一リンクにあるなら、両者ともH-a d d r を使って直接通信することができる。

【0129】(case4) case4では、case2と同様の処理を行う。ネットワーク42にデータパケット処理装置が設置されていれば、秘匿通信もcase2と同様に可能である。

【0130】(case5) case5では、case2と同様の処理を行う。

【0131】(case6) case6では、case3と同様の処理を行う。ネットワーク42にデータパケット処理装置が設置されていれば、秘匿通信もcase3と同様に可能である。

【0132】(case7~case10) case7~case10では、通信相手CHがデータパケット処理装置の設置されていないネットワーク43にあるので、秘匿通信は行わないものとする。また、通信相手CHは、組織外部のネットワークにいるので、移動ホストMHのH-a d d r を知らない点が前述のケースと異なっている。

【0133】case7~case10では、通信相手CHはパケットに移動ホストMHのM-a d d r を付けて送出する。その結果、パケットはネットワーク41のデータパケット処理装置45に到達する。この移動ホストMHのM-a d d r を付けたデータを受信すると(ステップS51)、データパケット処理装置45は移動ホストMHの3つ組アドレスを検索し、対応するC-a d d r でカプセル化して送出する(ステップS52)。その結果、パケットは移動ホストMHに転送される。

【0134】なお、case7では、データパケット処理装置45と移動ホストMHが同一のリンクにある場合は、移動ホストMHのC-a d d r をH-a d d r と同一に登録しておき、これを検出したら、カプセル化をせず、直接転送するようにすることもできる。

【0135】ここで、データ通信における「暗号化しないカプセル化」について説明する。FAを経由して暗号化情報を送る場合、FAは自組織に属す計算機とは限らないので、暗号化された内容は解読できない。従って、FA経由で送られるデータ内容は暗号化してカプセル化し、その外側を暗号化しないカプセル化してFAアドレスを付けて送る、という処理が必要である。このようにカプセル化されたデータの例を図11に示す。

【0136】以上説明したように、本発明に係る通信制御方法をMI Pに適用する場合、位置識別子記憶部内のC-a d d r として、pop-upモードは移動ホストMHが獲得したアドレスを登録し、FA使用モードではFAのアドレスを登録する。また、通信相手CHの位置が自組織ネットワーク内か否かにより通信相手CHが最初にデータパケットにつけるアドレスを変える。もし自組織ネットワーク内にいる通信相手CHからのメッセージならH-a d d r でアドレス付けされ、そうでなければM-a d d r でアドレス付けされているので、それに応じて必要なホームエージェントHAおよびデータパケット処理装置でアドレス群を検索しデータパケットを処理して行く。

【0137】この実施形態においては、H-a d d r , M-a d d r , C-a d d r を含むアドレス情報は、HA、ホームネットワークのデータパケット処理装置、FA、及び通信相手CHがパケット作成に使用する。従ってアドレス情報は、HA、またはホームネットワークのデータパケット処理装置に置いて、移動ノードからの登録メッセージに応じて内容を管理更新するか、FAに置いて移動ノードが訪問した際に情報をエントリする、などの方式で管理、操作できる。また通信相手CHについては、一般にどの移動計算機と通信するかが不明であるから、移動計算機のホームネットワークのHA、データパケット処理装置、または別途設定されたアドレス情報データベースに問い合わせてアドレス3つ組情報を得ることになる。

【0138】また、移動計算機がM-a d d r をどのように獲得するか、という点についても、以下のような方針が考えられる。

【0139】(1) ホームネットワークのHAがM-a d d r を複数管理しており、外部ネットワークに移動するMHに順次貸し出す。

【0140】(2) ホームネットワークのデータパケット処理装置がM-a d d r を複数管理しており、外部ネットワークに移動するMHに順次貸し出す。

【0141】(3) 訪問先のFAがM-a d d r を複数管理しており、移動してきたMHがグローバルアドレスを必要とする場合に貸し出す。

【0142】移動計算機がこれらのいずれかの方法でM-a d d r を獲得したら、システム内の全てのアドレス情報を新たに獲得したM-a d d r を含む最新の情報で更新することが必要である。

【0143】次に、VIPの実装例について説明する。

【0144】VIPは、日本のWIDEプロジェクトにてSony Computer Science Laboratory Inc. により提案された移動通信プロトコルであり、図12に示すように移動ホストMHに対する仮想的IPアドレス(VIP)と実際のIPアドレス(物理的位置に対応する)との対応関係を示す

情報(AMT 情報)を必要に応じて転送することで移動ホストへのルーティング情報を更新していく方式である。

【0145】各VIPルータ(VR)はAMT 情報を受けとり、対応するエントリを変えたり、更新したりして、移動ホストの移動、切断、登録などのイベントに対応する。VIPルータのうち、移動ホストMHが移動前にいたサブネットを管理するものをホームルータ(HR; 図12の79)という。

【0146】本発明をVIPに適用する際の、位置識別子記憶部の構成例を図13に示す。

【0147】VIPでは、MIPで用いられたlifetime(情報の有効期限)に加え、AMT 情報に付随するバージョン番号を管理することが必要になる。ここでは、位置識別子記憶部に新たにlifetimeおよびバージョン番号を示すフィールドを付けてこの管理を行う。以下の記載では、このような拡張された情報(AMT エントリ)を全てのVIPルータが保持、管理するものとする。

【0148】VIPでは、MIPのpop-upモードと同様に、移動ホストMHがネットワークレイヤのインターネットアドレスを得た上で通信を行う(文献: R. Droms: "Dynamic Host Configuration Protocol", IETF-RFC1541, Oct. 1993)。この場合、仮想的に定めたVIPアドレスと、移動ホストMHが獲得したインターネットアドレス(IPアドレス)との対応関係をAMT 情報として伝搬させる。

【0149】本発明に係る通信制御方法をVIPに適用する場合は、VIPアドレスとしてH-addrまたはM-addrを、IPアドレスとしてはC-addrを対応づけし、これに従って各制御、通信動作を行っていく。本発明の3つの位置識別子を含むテーブルは、ホームルータHR、全てのVIPルータ(またはそれに相当する動作を行う装置)、全てのホストが保持するものと仮定する。

【0150】以下、VIPの各動作を説明する。

【0151】(1) VIPの登録

ホームの自組織ネットワーク外に移動した移動ホストMHは、登録を行なうために、AMT 作成メッセージをホームルータHR宛に出す。AMT 作成メッセージ内には、3つ組アドレス、その他の必要な情報が入る。

【0152】途中のVIPルータは、AMT 作成メッセージを受けとったら、自身の保持する情報を更新するとともに、サブネット内にメッセージをブロードキャストする。

【0153】ホームルータHRは、ホーム・サブネット(Home Subnet)内にAMT エントリ(3つ組アドレス)をブロードキャストする。また、ホームルータHRは、AMT エントリの消去禁止ビット(テー

ルに附属するビットフィールドとして実装)を立てる。

【0154】(2) VIPのkeep-alive
移動ホストMHは、再登録を行うために、ホームルータHRのAMT エントリの保持期限より短い周期でAMT 作成メッセージをホームルータHRに再送する。

【0155】ホームルータHRは、ホーム・サブネット内にAMT エントリを再度ブロードキャストする。

【0156】(3) VIPの切断

移動ホストMHは、切断を行なう場合、AMT 無効メッセージをホームルータHRに送信する。

【0157】AMT 無効メッセージを受信したホストはエントリの無効フラグを立てる。

【0158】無効化されたエントリに対応するパケットがこのホスト/ルータを通ったら、パケットの中味をみてそのアドレスマッピングを行なったホスト/ルータにAMT 無効メッセージを流す。

【0159】(4) VIPの移動

移動ホストMHが移動して新しいネットワークに接続したら、ホームルータHRにAMT 作成メッセージを再送する。

【0160】途中のルータでAMT 作成メッセージを受信したら、対応するエントリを更新する。

【0161】ホームルータHRにAMT 作成メッセージが到着したら、ホーム・サブネット内にそのAMT エントリをブロードキャストし、移動ホストMHが前にいたネットワークのルータにもAMT 作成メッセージを流す。

【0162】前にいたネットワークのルータは、自分のAMT エントリを書換え、それまで登録されていた古いAMT エントリを使って送信されたパケットを新AMT のアドレスに転送し、さらに無効となったMTをマッピングしたホスト/ルータにAMT 無効メッセージを流す。

【0163】(5) VIPのデータ通信

VIPのデータ通信の方法について図14を参照して説明する。この場合も、原則として、移動ホストMHへのアドレッシングは、プライベートアドレスを共有する同一組織内ではH-addrで行い、それ以外の外部組織にある移動ホストに対してはM-addrで行う。

【0164】図14にVIPを使った移動通信をサポートするネットワーク構成を示す。ネットワーク91は、移動ホストMHが本来接続されていたホームネットワークである。ネットワーク92は外部ネットワークであるがネットワーク91と同じ組織に管理されており、互いに共通のプライベートアドレスで各ホストを一意にアドレッシング可能であるとする。ネットワーク93、94は外部組織のネットワークである。ネットワーク91の出口と移動ホストに附属してデータパケット処理装置95、96が設置されており、秘匿通信(暗号化通信)をサポートするものとする。

【0165】以下、VIPの通信動作を通信相手CH、移動ホストMHの位置関係によって場合分けし、図15、図16の動作フローチャートを参照しながら説明する。

【0166】通信相手CHと移動ホストMHの位置関係は、次の10のケースが考えられる。

【0167】cace1は、通信相手CHの位置がネットワーク91内で、移動ホストMHの位置がネットワーク91の場合である。

【0168】cace2は、通信相手CHの位置がネットワーク91内で、移動ホストMHの位置がネットワーク92の場合である。

【0169】cace3は、通信相手CHの位置がネットワーク91内で、移動ホストMHの位置がネットワーク93の場合である。

【0170】cace4は、通信相手CHの位置がネットワーク92内で、移動ホストMHの位置がネットワーク91の場合である。

【0171】cace5は、通信相手CHの位置がネットワーク92内で、移動ホストMHの位置がネットワーク92の場合である。

【0172】cace6は、通信相手CHの位置がネットワーク92内で、移動ホストMHの位置がネットワーク93の場合である。

【0173】cace7は、通信相手CHの位置がネットワーク93内で、移動ホストMHの位置がネットワーク91の場合である。

【0174】cace8は、通信相手CHの位置がネットワーク93内で、移動ホストMHの位置がネットワーク92の場合である。

【0175】cace9は、通信相手CHの位置がネットワーク93内で、移動ホストMHの位置がネットワーク93の場合である。

【0176】cace10は、通信相手CHの位置がネットワーク93内で、移動ホストMHの位置がネットワーク94の場合である。

【0177】図15は、上記のcace1～cace6の場合の動作である。

【0178】図16は、上記のcace7～cace10の場合の動作である。

【0179】(cace1～cace3) cace1～cace3では、通信相手CHは、移動ホストMHに対するAMT情報を持っているなら(ステップS61 YES)、宛先を移動ホストMHのC-addrとしてパケットを送出する(ステップS64)。

【0180】一方、通信相手CHが移動ホストMHに対するAMT情報を持っていない場合(ステップS61 NO)は、宛先を移動ホストMHのH-addrとして送出する(ステップS62)。この場合、パケットはホームルータHRに向けて送出される。途中のVIPルー

タでは、AMTエントリを調べ、移動ホストMHのH-addrに対応するC-addrに宛先アドレスを付け替えて転送する(ステップS63)。

【0181】ここで、両者が秘匿通信を行う場合は、最初のC-addrでのカプセル化の前に暗号化する。

【0182】なお、cace1では、両者ともC-addrを使って直接通信することができる。

【0183】(cace4) cace4では、cace2と同様の処理を行う。ネットワーク92にデータパケット処理装置が設置されていれば、秘匿通信もcace2と同様に可能である。

【0184】(cace5) cace5では、cace2と同様の処理を行う。ただし、両者が同一のネットワーク上にいるので、それが認識できれば直接H-addrで通信するように最適化することができる。

【0185】(cace6) cace6では、cace3と同様の処理を行う。ネットワーク92にデータパケット処理装置が設置されていれば、秘匿通信もcace3と同様に可能である。

【0186】(cace7～cace10) cace7～cace10では、通信相手CHがデータパケット処理装置の設置されていないネットワーク93にあるので、秘匿通信は行わないものとする。また、通信相手CHは、組織外部のネットワークにるので、移動ホストMHのH-addrは知らない点が前述のケースと異なっている。

【0187】cace7～cace10では、通信相手CHは移動ホストMHに対するAMT情報を持っているなら(ステップS71 YES)、宛先を移動ホストMHのC-addrとしてパケットを送出する(ステップS74)。

【0188】一方、通信相手CHが移動ホストMHに対するAMT情報を持っていない場合は(ステップS71 NO)、宛先を移動ホストMHのM-addrとして送出する(ステップS72)。

この場合、パケットはホームルータHRに向けて送出される。途中のVIPルータでは、AMTエントリを調べ、移動ホストMHのM-addrに対応するC-addrに宛先アドレスを付け替えて転送する(ステップS73)。

【0189】ここで、上記の全ケースにおいて、通信相手CHが移動ホストMHに対する有効なAMT情報を持たない場合(移動ホストMHのC-addrを含んだAMT情報がまだ通信相手CHに到達していない場合)がある。

【0190】そのような場合は、通信相手CHは、H-addr/M-addr(VIPaddress)を宛先としたパケットを送出する。その結果、パケットはホームルータHRに向かって送られる。

【0191】途中のVIPルータの内、AMTバージョンの同じルータは正しい宛先にパケットのアドレスをつ

けかえて送信する。ルータのAMTバージョンがパケットのそれより古い場合は自分のAMTエントリに無効フラグを立てる。ルータのAMTバージョンがパケットのそれより新しいルータはデータパケットのAMTエントリを更新して新しい行き先に送る。

【0192】また、通信相手CHから移動HOST MHへのパケット転送の途中の各VIPルータにおいても、ルータのAMTバージョンがパケットのそれより古い場合は自分のAMTエントリに無効フラグを立てる。ルータのAMTバージョンがパケットのそれより新しいルータはデータパケットのAMTエントリを更新して新しい行き先に送る、という制御を行う。

【0193】つまり、VIPにおいては、通信相手CHは最初VIPアドレスであるH-a d d r /M-a d d r でアドレスをつけてパケットを投げる(もし、全てのVIPルータが移動HOST MHのAMT情報を持たなければ、そのパケットはホームルータHRまで到達する)。そのパケットは転送途中の移動HOST MHに関するAMT情報を保持するVIPルータでアドレスをC-a d d r に変換され、移動HOST MHの現在位置に向かってルーティングされるようになる。

【0194】以上、説明したように、現在様々提案されている移動通信プロトコルに対して、本発明を適宜適用することでその定義を逸脱することなく容易に実現が可能である。

【0195】また、本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0196】

【発明の効果】本発明によれば、移動計算機の移動箇所に応じて2種類のアドレス(計算機に固有の自組織ネットワーク内で一意に定められた第1の位置識別子と、ネットワーク上の位置を変更して通信を行う計算機に予約されたネットワーク全体で一意に定められた第2の位置識別子)を切替えて使用するようにしたので、従来のように全てのネットワーク上で一意なアドレスを全て移動計算機に与え貴重な外部ネットワークアドレスを浪費するようなことなく、移動通信のサポートが可能となる。

【0197】また、本発明によれば、移動計算機がネットワーク間を移動する場合、移動計算機の情報が更新される場合、移動計算機の情報が無効化される場合など様々な制御情報に対応可能であり、その結果様々な移動プロトコルにも柔軟に対応可能な移動通信環境を提供できる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るネットワークの基本構成を示す図。

【図2】同実施形態に係る通信制御における位置識別子

記憶部の一構成例を示す基本構成図。

【図3】IETF/Mobile-IPにおけるネットワーク構成を示す図。

【図4】本発明をIETF/mobile-IPに適用した実施形態における位置識別子記憶部の一構成例を示す基本構成図。

【図5】本発明をIETF/mobile-IPに適用した実施形態におけるネットワーク構成の例を示す基本構成図。

【図6】FAモードにおける処理手順を示すフローチャート。

【図7】FAモードにおける処理手順を示すフローチャート。

【図8】FAモードにおける処理手順を示すフローチャート。

【図9】pop-upモードにおける処理手順を示すフローチャート。

【図10】pop-upモードにおける処理手順を示すフローチャート。

【図11】本発明をIETF/mobile-IPに適用した実施形態における外部エージェント経由で転送されるデータパケットの形式の一例を示す図。

【図12】VIPにおけるネットワーク構成を示す図。

【図13】本発明をVIPに適用した実施形態における位置識別子記憶部の一構成例を示す基本構成図。

【図14】本発明をVIPに適用した実施形態におけるネットワーク構成の例を示す基本構成図。

【図15】VIPにおける処理手順を示すフローチャート。

【図16】VIPにおける処理手順を示すフローチャート。

【符号の説明】

1 a, 3 1, 4 1, 7 1, 9 1 自組織ネットワーク

1 b, 4 2, 9 2 外部の自組織ネットワーク

1 c, 4 3, 4 4, 9 3, 9 4 外部組織ネットワーク

1 d, 4 7, 7 2, 7 3, 7 4, 9 7 外部ネットワーク

2, 5 1, 1 0 2 計算機

2 1, 5 6, 1 1 2 移動計算機

3 a, 3 b, 4 5, 4 6, 9 5, 9 6 データパケット処理装置

3 2, 3 3, 3 4 外部ネットワーク

3 5, 5 2 ホームエージェント

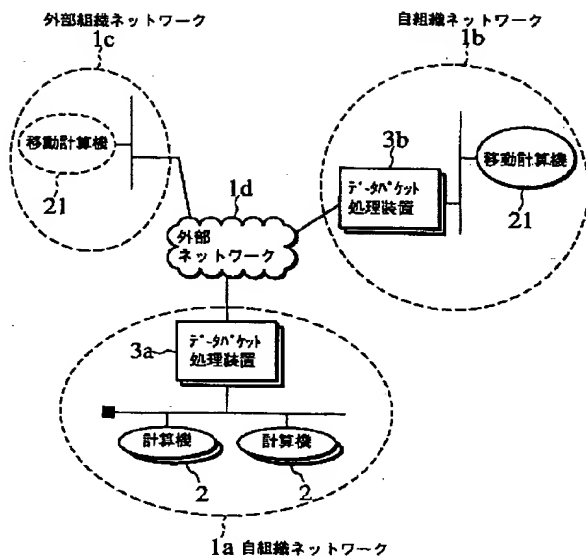
3 6, 5 3, 5 4, 5 5 外部エージェント

7 5, 7 6, 7 7, 7 8, 1 2 1, 1 2 2, 1 2 3, 1

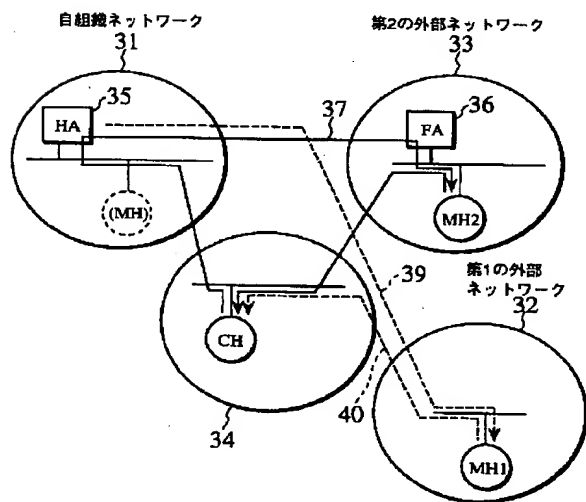
2 4 VIPルータ

7 9, 9 2 ホームルータ

【 図1 】



【 図3 】



【 図13 】

Home address (H-addr)
Mobile address (M-addr)
Care-of address (C-addr)
Lifetime value
Version number

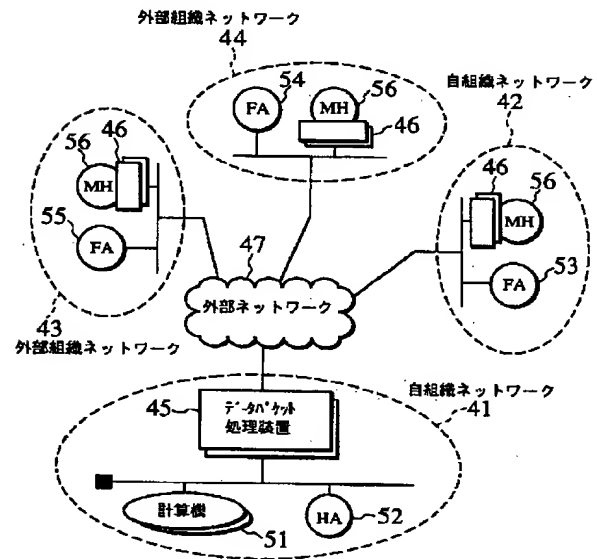
【 図2 】

Home address (H-addr)
Mobile address (M-addr)
Care-of address (C-addr)

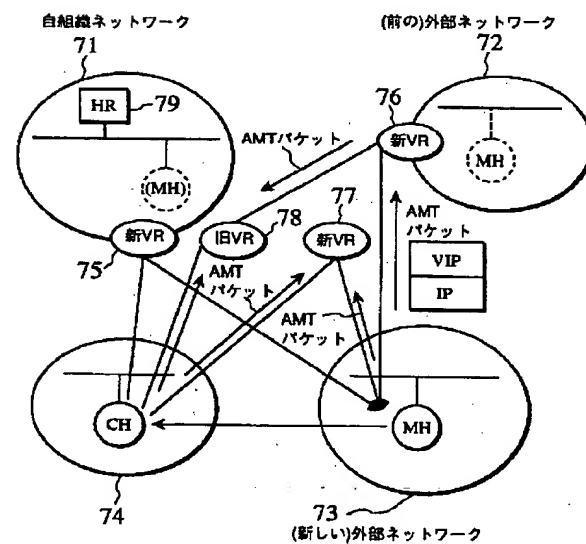
【 図4 】

Home address (H-addr)
Mobile address (M-addr)
Care-of address (C-addr)
Lifetime value

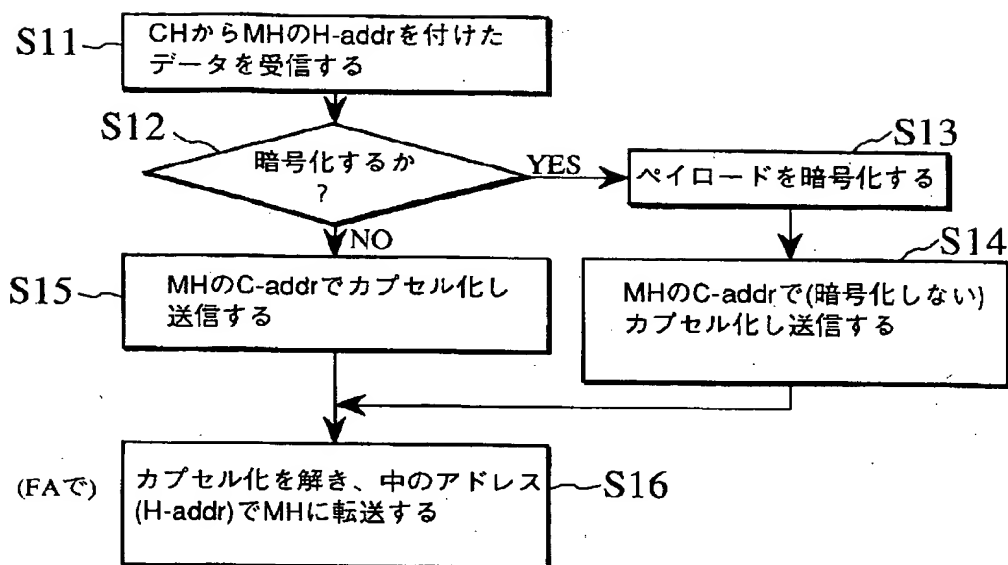
【 図5 】



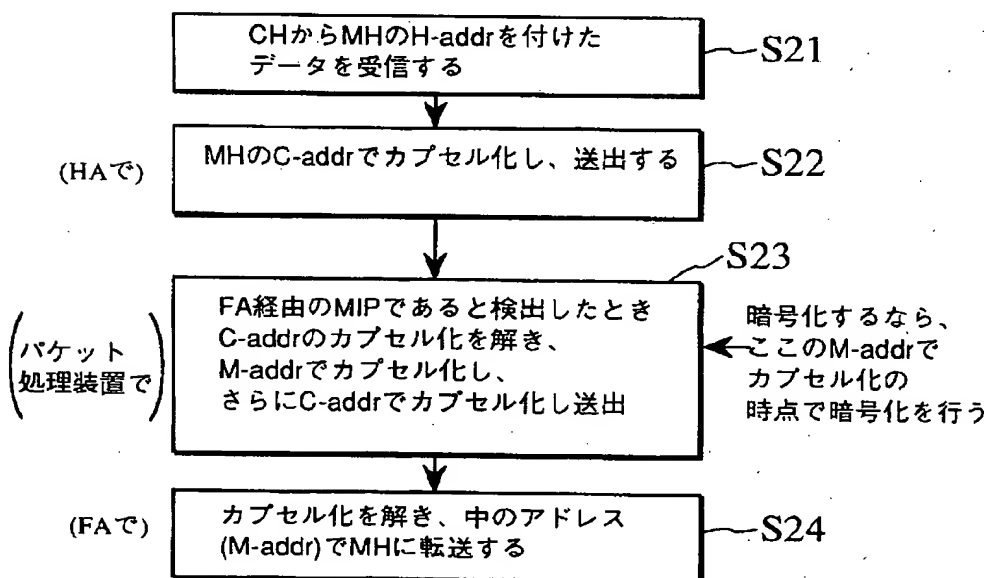
【 図12 】



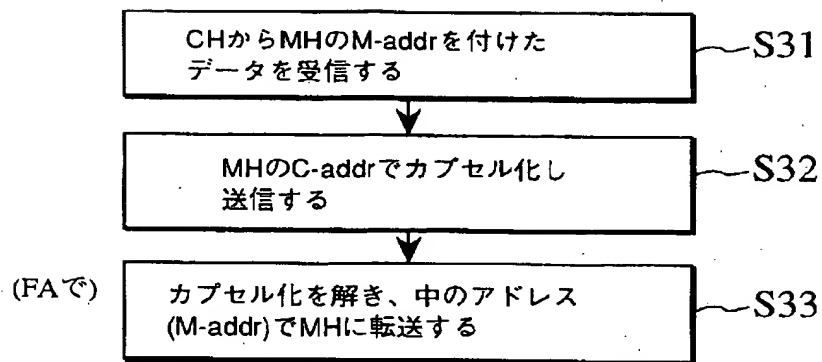
【 図6 】



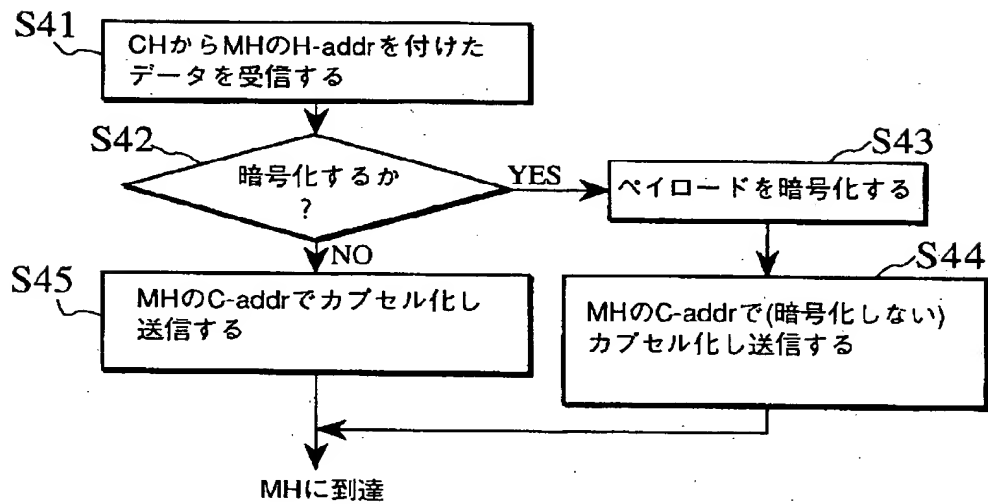
【 図7 】



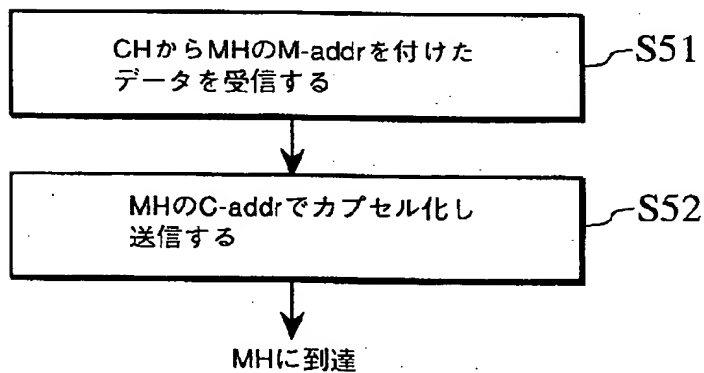
【 図8 】



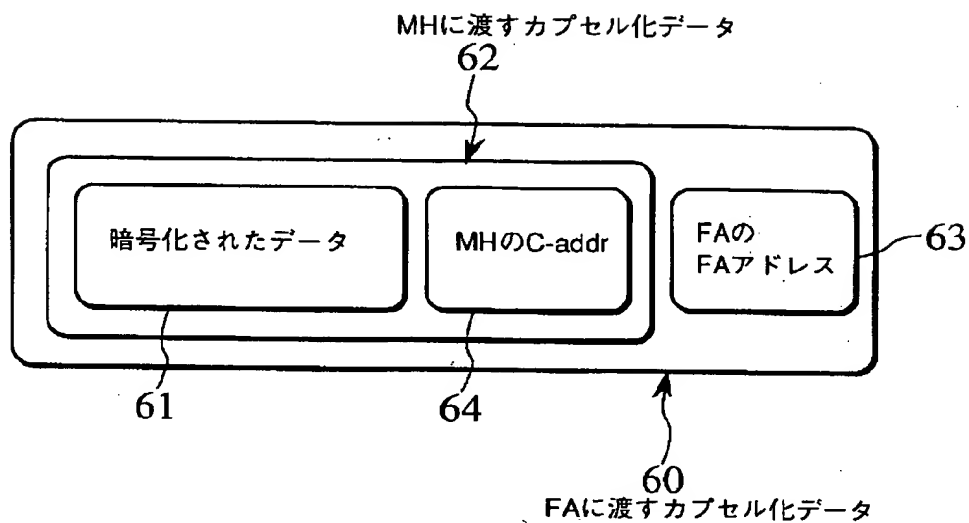
【 図9 】



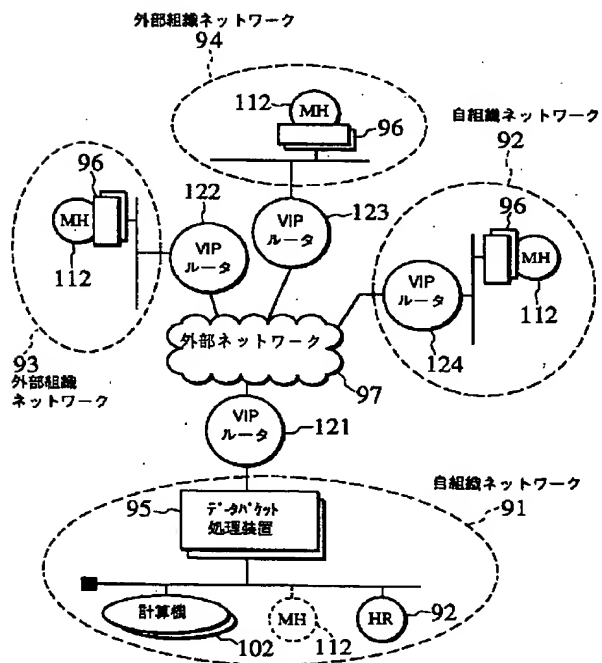
【 図10 】



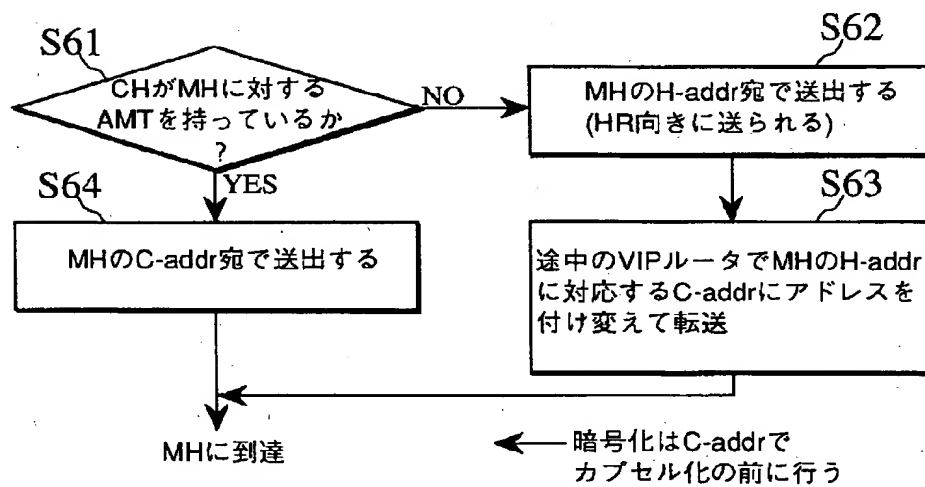
【 図1 1 】



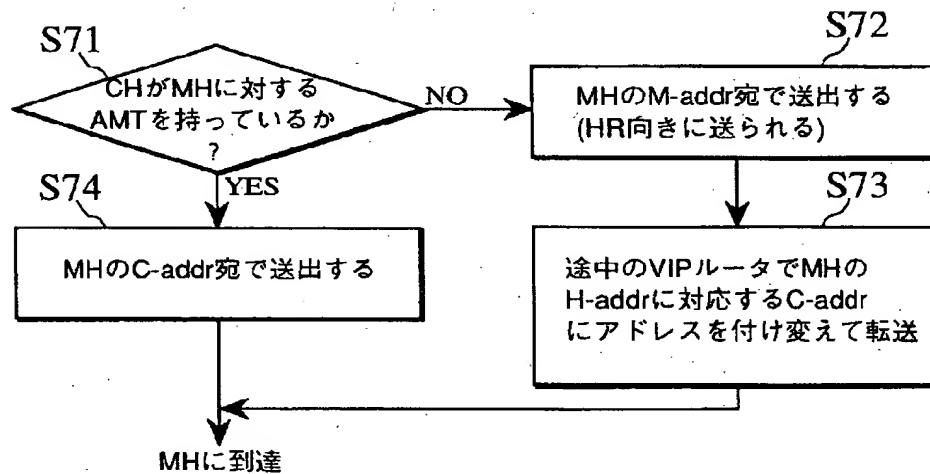
【 図1 4 】



【 図1 5 】



【 図1 6 】



フロント ページの続き

(72)発明者 新保 淳
神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内

(72)発明者 岡本 利夫
神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内